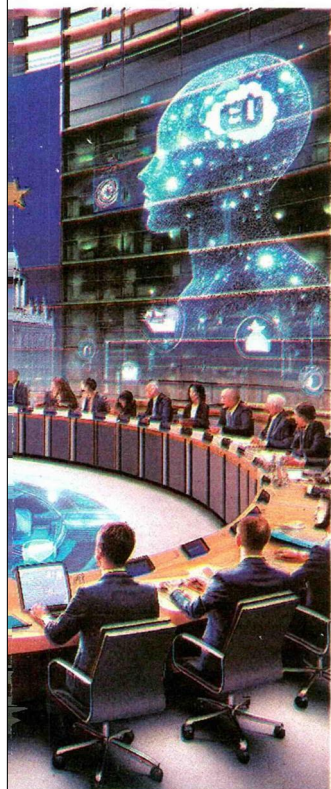




PROHIBIDA SU REPRODUCCIÓN Y/O DIFUSIÓN

Inteligencia Artificial en la Unión Europea



significativos.

Por otra parte, incorpora sistemas de categorización biométrica que infieran atributos sensibles (raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida u orientación sexuales), excepto el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente o cuando las fuerzas de seguridad categoricen datos biométricos.

Contemplan también sistemas de puntuación social, es decir, evaluar o clasificar a individuos o grupos basándose en comportamientos sociales o rasgos personales, causando un trato perjudicial o desfavorable a esas personas.

IA PREDICTIVA

La norma incluye dentro de los prohibidos a los sistemas de IA para evaluar el riesgo de que un individuo cometa delitos penales basándose únicamente en perfiles o rasgos de personalidad, excepto cuando se utilice para aumentar las evaluaciones humanas basadas en hechos objetivos y verificables directamente relacionados con la actividad delictiva.

La compilación de bases de datos de reconocimiento facial mediante el raspado no selectivo de imágenes de Internet o de

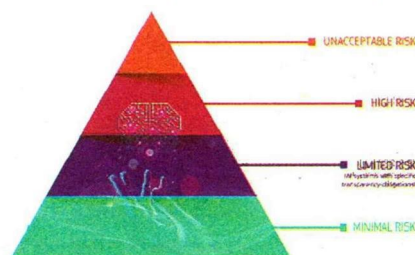
grabaciones de CCTV; inferir emociones en lugares de trabajo o centros educativos, salvo por razones médicas o de seguridad.

También la identificación biométrica remota (RBI) en tiempo real en espacios de acceso público para las fuerzas de seguridad con condiciones excepto en: a) caso de búsqueda de personas desaparecidas, víctimas de secuestros y personas víctimas de la trata de seres humanos o la explotación sexual; b) prevenir una amenaza sustancial e inminente para la vida, o un ataque terrorista previsible; c) identificar a sospechosos de delitos graves.

DEFINICIÓN ALTO RIESGO

Según la CE los sistemas de IA se consideran siempre de alto riesgo si realizan perfiles de las personas, es decir, el tratamiento automatizado de datos personales. Esto incluye a los que se utilizan para evaluar diversos aspectos de la vida de una persona, como su rendimiento laboral, su situación económica, su salud, sus preferencias, sus intereses, su fiabilidad, su comportamiento, su ubicación o sus movimientos.

También son de alto riesgo los sistemas que utilizan como componente de seguridad o producto



cubierto por la legislación de la UE; asimismo aquellos incorporados en lista específica relativos a algunos sistemas que trabajen con datos biométricos; infraestructuras críticas; educación y formación profesional; empleo, gestión de trabajadores y acceso al autoempleo; acceso y disfrute de los servicios privados esenciales y de los servicios y prestaciones públicas esenciales; fuerzas y cuerpos de seguridad; gestión de la migración, el asilo y el control de fronteras; y sobre la administración de justicia y procesos democráticos.

REQUISITOS ALTO RIESGO

Según la ley los proveedores de IA de alto riesgo deben cumplir un conjunto de normas: a) establecer un sistema de gestión de riesgos a lo largo del ciclo de vida del sistema de IA de alto riesgo; b) llevar a cabo la gobernanza de los datos, garantizando que los conjuntos de datos de formación, validación y prueba sean pertinentes, suficientemente representativos y, en la medida de lo posible, estén libres de errores y completos de acuerdo con la finalidad prevista.

Luego, c) elaborar documentación técnica para demostrar la conformidad y facilitar a las autoridades la información necesaria para evaluar dicha conformidad;

d) diseñar su sistema de IA de alto riesgo para que pueda registrar automáticamente los eventos relevantes para identificar los riesgos a nivel nacional y las modificaciones sustanciales a lo largo del ciclo de vida del sistema; e) proporcionar instrucciones de uso a los encargados de la implantación posterior para permitir el cumplimiento por parte de estos últimos.

Por último, f) diseñar su sistema para permitir a los desplegados aplicar la supervisión humana; g) diseñar su sistema para alcanzar los niveles adecuados de precisión, solidez y ciberseguridad; h) establecer un sistema de gestión de la calidad para garantizar el cumplimiento.

GOBERNANZA

De acuerdo con la ley se creará la Oficina Europea de AI, dependiente de la CE, para supervisar la aplicación efectiva y el cumplimiento de las normas establecidas conjuntamente con los gobiernos nacionales que la aplicarán. Asimismo, se creará el Consejo Europeo de IA que estará compuesto por un representante de cada Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. El Consejo asesorará y asistirá a la CE y a los Estados miembros para facilitar la aplicación coherente y eficaz de la ley.

La Oficina de AI también

asistirá a las reuniones del Consejo sin tomar parte en las votaciones. El Consejo podrá invitar a las reuniones, caso por caso, a otras autoridades, organismos o expertos nacionales y de la Unión, cuando las cuestiones debatidas sean pertinentes para ellos.

El Consejo establecerá dos subgrupos permanentes para proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y las autoridades notificantes sobre cuestiones relacionadas con la vigilancia del mercado y los organismos notificados, respectivamente.

EVALUACIÓN Y REVISIÓN

La CE evaluará la necesidad de modificar la lista de prácticas de IA prohibidas y de alto riesgo una vez al año tras la entrada en vigor de la ley y hasta el final del periodo de delegación de poderes. La CE presentará los resultados de dicha evaluación al Parlamento Europeo y al Consejo.

A más tardar tres años después de la fecha de aplicación de la presente ley, y posteriormente cada cuatro años, la CE presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión de la ley. Dicho informe incluirá una evaluación de la estructura de la aplicación y de la posible necesidad de crear una agencia de la Unión para resolver las deficiencias detectadas. Por último, se establecen otras fechas para ir actualizando y mejorando diferentes aspectos particulares de la norma.

para distorsionar el comportamiento y perjudicar la toma de decisiones con conocimiento de causa, causando un daño significativo. Asimismo, explotar las vulnerabilidades relacionadas con la edad, la discapacidad o las circunstancias socioeconómicas para distorsionar el comportamiento, causando daños